

Applicant : Sweet et al.
Atty Dkt. : 00131-000100000
Issued : n/a
Serial No. : 09/930,029
Filed : 08/14/2001
Page : Page 15 of 28

REMARKS

Applicants wish to thank the Examiner for meeting and discussing this case March 9, 2009. During the meeting and as noted in the Interview Summary, the Examiner requested clarification that Scheidt taught physically giving smart cards with credentials to users as evidence of teaching away from using an intranet or Internet to deliver the same over a network. In light of our discussion, the Applicants have prepared this supplemental amendment to the response filed March 10, 2009 and included the attached declaration and corresponding remarks herein below.

In the Office Action mailed October 10, 2008, the Examiner objected to Claims 66 and 67 as duplicative. Accordingly, Claim 67 was canceled in order to address this informality and not to overcome any cited art.

Further, the Examiner rejected Claims 4-6, 15-22, 57, 58, and 63 under 35 USC 112, first paragraph as failing the written description requirement. In particular, the Examiner asserts that "Claim 4 recites in the final limitation that the working key will allow the network user to 'decrypt other than the selected portions of the encrypted object'" and that there "is no basis in the specification for this 'other than' portion of the claim." (Office Action, page 3, paragraph 1) Applicants submit this language was a typographical informality and have removed 'other than' from the respective claim 4 and claim 63. Withdrawal of the rejection is respectfully requested.

Applicant : Sweet et al.
Atty Dkt. : 00131-000100000
Issued : n/a
Serial No. : 09/930,029
Filed : 08/14/2001
Page : Page 16 of 28

Claims 52-58 were rejected under 35 USC 101 as directed towards non-statutory subject matter due to a lack of physical components. Applicants have revised Claim 52 to include physical components of “at least one processor associated with the system” and address this concern. No new matter has been added and withdrawal of this rejection is respectfully requested.

Regarding substantive rejections, the Examiner rejected Claim 1-20, 52-57 and 59-67 under 35 USC 103(a) in view of Scheidt (US Pat. 6,490,680) in view of He (US Pat. 6,088,451) and Shanton (US Pat. 5,680,452). The Examiner broadly referenced several portions of Scheidt with respect to Claim 1 yet admitted that Scheidt does not operate by “securely transmitting the access permission security profile to the network user over the network wherein the ephemeral cryptographic characteristic allows the network user in receipt of the access permission security profile to perform cryptographic operations for a predetermined period of time” as recited in Claim 1. Unfortunately, Scheidt alone or in combination with the He and/or Shanton do not teach or even suggest these aspects of the invention as claimed. For at least this reason, the Examiner has failed to establish a prima facie case for rejecting Claim 1. Under MPEP §2143 Basic Requirements of a Prima Facie Case of Obviousness specifies:

“To establish a prima facie case of obviousness, three basic criteria must be met. First, there must be some suggestion or motivation, either in the references themselves or in the knowledge generally available to one of ordinary skill in the art, to modify the reference or to combine reference teachings. Second, there must be a reasonable expectation of success. Finally, the prior art reference

Applicant : Sweet et al.
Atty Dkt. : 00131-000100000
Issued : n/a
Serial No. : 09/930,029
Filed : 08/14/2001
Page : Page 17 of 28

(or references when combined) must teach or suggest all the claim limitations. The teaching or suggestion to make the claimed combination and the reasonable expectation of success must both be found in the prior art, not in applicant's disclosure. In re Vaeck , 947 F.2d 488, 20 USPQ2d 1438 (Fed. Cir. 1991)”

Accordingly, the Applicants respectfully requests that the Examiner withdraw the rejection under 35 USC 103(a) for failing to teach or suggest each and every claim limitation.

First, it is not clear that Scheidt or other cited references teach or suggest any of the limitations in Claim 1. For example, Scheidt fails to disclose “receiving a request for an access permission security profile on behalf of a network user” as recited in claim 1. Contrary to the Examiner’s assertion, no where does Scheidt indicate that a network user makes any requests for the access permission security profile. Instead, Scheidt insists that either a smart card (Col. 11, lines 24-30) or a super card (Col. 11, lines 65-67; Col. 12, lines 1-11) should be used store and hold this information and be directly connected to a workstation (i.e., not accessed over a network). There is no request for the access permission security profile since it is already stored in the smart card attached directly to the workstation (Col. 5, lines 65-67; Col. 6, lines 1-6; Col. 10, lines 28-42).

Moreover, Scheidt suggests and therefore teaches away from using anything but a smart card . Specifically, Scheidt extolls the virtue of centralizing more tasks to the super card rather than less. It is the teachings, suggestions and belief of Scheidt that placing more functions on the smart

Applicant	:	Sweet et al.
Atty Dkt.	:	00131-000100000
Issued	:	n/a
Serial No.	:	09/930,029
Filed	:	08/14/2001
Page	:	Page 18 of 28

card will inherently increase the overall security of the CKM system because “local processing within the card increases the workload of an adversary who is trying to snoop the internal workings” of CKM (Col. 12, lines 1-11). In fact, Scheidt neither recognizes or mentions any of the pitfalls of requiring a physical smart card to perform CKM hence there is clearly no motivation to eliminate this aspect of Scheidt or combine with any other approach.

For example, Scheidt intentionally requires that the card having the credentials be handed to the user directly as part of a security measure. (Col. 9, lines 60-63) Indeed, the additional act of reissuing new credentials must also occur by requiring a manual update of the smart card or other storage device back with an administrator. (Col. 10, 14-19)

Scheidt could also not possibly teach or suggest “creating the access permission security profile to form a cryptographic key for enabling the network user to decrypt selected portions of an encrypted object when one or more groups associated with the encrypted object match the network user’s membership in one or more groups within the domain and to encrypt selected portions of a plaintext object to be accessed by other network users when the other network user’s membership in one or more groups within the domain also match the one or more groups associated with the selected portions of the plaintext object being encrypted” as recited in Claim 1. First, Scheidt assumes the smart card already has the access permission security profile hence there is no

Applicant	:	Sweet et al.
Atty Dkt.	:	00131-000100000
Issued	:	n/a
Serial No.	:	09/930,029
Filed	:	08/14/2001
Page	:	Page 19 of 28

reason to then create it on demand since “the Credential Manager will initialize a smart card with that user’s ID” and the “[the] card is then given to the user.”(Col. 9, lines 39-43). In distinct comparison, the access permission security profile in Scheidt is created in advance and not on demand as recited in Claim 1.

Further, Scheidt does not teach or suggest “securely transmitting the access permission security profile to the network user over the network” as recited in claim 1. By design, Scheidt stores the access permission security profile on the smart card or super card in advance and then gives the smart card to the user. Once again, Scheidt neither teaches nor suggests this aspect of the invention as recited in claim 1.

The Examiner admits that Schiedt does not teach or suggest all of Claim 1 and relies, instead upon He. The Examiner incorrectly asserts that He teaches or suggests, “receiving a request for an access permission security profile on behalf of a network user” as recited in Claim 1. To combine He with Schiedt would defeat the security aspect of Schiedt requiring that the smart card, super card or other storage device must be used to hold an access permission security profile. (Col. 10, lines 28-31)

Applicants declaration attached herein also indicates that the above construction of Schiedt is correct and strongly teaches away from using anything other than a smart card issued in person or

Applicant : Sweet et al.
Atty Dkt. : 00131-000100000
Issued : n/a
Serial No. : 09/930,029
Filed : 08/14/2001
Page : Page 20 of 28

through the mail. By way of this declaration, the Examiner should find that that the Scheidt patent appears to only provide for an in-person authentication followed by a manual distribution of a smart card with newly created credentials. On Col. 9, lines 39-55, the Scheidt patent describes that “the card is then given to the user” and “It is preferable that the user is present at this step, or that a method is used to assure the user’s identity.” The Scheidt patent does teach that the smart card with credentials should be handed over to a person only if they have been properly authenticated in-person. Conversely, the Scheidt patent teaches away from the credentials being transmitted over an intranet or the Internet.

The declaration should also convince the Examiner that updated or reissued credentials may be distributed without in-person authentication by a Credentials Manager but still not over a network or the Internet. Indeed, the Scheidt patent states that someone other than the Credentials Manager may give the new credentials to a user since the user has already been authenticated previously. (Col. 10, lines 20-23 of the Scheidt patent) However, passwords may be sent over an organizational administrative channel but not over the Internet. (Col. 10, lines 24-26 of the Scheidt patent) Organizational administrative channels might use inter-office mail pouches, USPS or courier. The organizational administrative channels in the Scheidt patent do not include a network

Applicant	:	Sweet et al.
Atty Dkt.	:	00131-000100000
Issued	:	n/a
Serial No.	:	09/930,029
Filed	:	08/14/2001
Page	:	Page 21 of 28

or the Internet. If the Scheidt patent had intended to include a network as part of the distribution then they would have expressly specified this as a possible solution—this of course is not the case.

Even if it were proper to combine Scheidt with He, the result would not correspond to the limitations as recited in Claim 1.

First, He concerns controlling access to “network elements” and does not teach or suggest anything about requesting and receiving access permission security profiles. For example, He states, “The central theme around security of network elements is how user access can be appropriately and effectively controlled for access to network elements.” (He, Col 5, lines 4-7) Network elements according to He are defined as “switches, signaling transfer points (STPs), data access points (DAPs), mainframe computers” but mentions nothing about access permission security profiles. If all goes well, He provides a “list of user credentials” necessary for subsequently “requesting access to network resources and information” but does not actually provide direct access to anything. (He, Col. 19, lines 32-35) Unlike an access permission security profile, the “list of user credentials” does not allow encryption or decryption of objects to occur.

Second, the Examiner has asserted that other elements of Claim 1 are obvious yet has provided no basis for these facts in Scheidt, He or even Shanton. For example, the Examiner states, “It would have been obvious to one of ordinary skill in the art at the time of applicant’s invention to

Applicant : Sweet et al.
Atty Dkt. : 00131-000100000
Issued : n/a
Serial No. : 09/930,029
Filed : 08/14/2001
Page : Page 22 of 28

incorporate the security system of He into the access control system of Schiedt in order to provide a mechanism by which a user can request creation and/or transmission of his or her security profile while ensuring that the user is authentic and authorized before sending such profile, such that the profile can be stored securely on a central server and accessed by the user from a variety of different devices.” (Office Action October 10, 2008, page 6, lines 9-16). With all due respect, the Applicants can find no basis for such a detailed assertion in He or any other cited references. Accordingly, Applicants would respectfully request the Examiner to withdraw the rejection if the source of these many limitations cannot be specifically identified.

It should also be appreciated that He very strongly teaches away from making any assumptions about network security unless they are expressly stated. Indeed, He stands for teaching away from the Examiner or others making assumptions about complex security mechanisms. He reflects the general notion present at the time of the invention that security systems cannot rely upon

Applicant : Sweet et al.
Atty Dkt. : 00131-000100000
Issued : n/a
Serial No. : 09/930,029
Filed : 08/14/2001
Page : Page 23 of 28

an interconnect but instead should use hardware solutions that can be physically secured. According to He,

The security of the interconnection network that enables users to access network resources and information in the network elements shall never be automatically assumed in any comprehensive solution to the protection of network resources and information. This is simply because it is impossible to physically secure each and every single link of the network.

(He, Col. 7, lines 41-45)

Based on what He does actually teach, it would fall to reason that the Examiner cannot assume anything about network security (at the time of the invention thereof) when it involves a user accessing network resources and information. Moreover, He expresses that those skilled in the art at the time of this invention generally were concerned about ensuring physical security and were definitely not comfortable separating secure components from hardware. One skilled in the art at the time of He would most definitely not consider actually sending an access permission security profile to a user over a network, especially the Internet, as that would not ensure physical security.

It is also interesting to note that He also teaches away from ever taking any password information, authentication data off of a hardware solution such as the smart card used in Scheidt. Specifically, He also states,

In addition, no attempts to secure the interconnection network shall ever be pursued, for they are never be achievable except in very

Applicant : Sweet et al.
Atty Dkt. : 00131-000100000
Issued : n/a
Serial No. : 09/930,029
Filed : 08/14/2001
Page : Page 24 of 28

few isolated instances where the inter-connection network can be physically constrained in an area where physical security can be assured. This is definitely not the situation for many large enterprise networks.

(He, Col. 7, lines 49-54)

Based on this further aspect of what He does teach, it would follow that access permission security profiles should never be separated from a smart card or transmitted over the Internet. Those skilled in the art at the time of He believed that no security was possible over a network unless physical security were somehow assured. Taking Schiedt in view of He, one skilled in the art would not attempt to send a access permission security profile over the Internet or other network since it would not be possible to assure physical security along the way. If anything, He teaches away from transmission of a security profile over a network.

Applicants respectfully request withdrawal of the rejection for Claim 1 because the Examiner has failed to show each and every element in Scheidt, He and/or Shanton.. Independent Claims 4,7, and 52 remain patentable for at least the reasons provided with respect to Claim 1. Dependant claims 2-3, 5-6 and 8-22, 53-66 while allowable on their own, also are in condition for allowance for at least the same reasons specified with respect to their corresponding independent

Applicant : Sweet et al.
Atty Dkt. : 00131-000100000
Issued : n/a
Serial No. : 09/930,029
Filed : 08/14/2001
Page : Page 25 of 28

parent claims. ("If an independent claim is nonobvious under 35 U.S.C. 103, then any claim depending therefrom is nonobvious." *In re Fine*, 837 F.2d 1071, 5 USPQ2d 1596 (Fed. Cir. 1988)).

The Examiner has also rejected 52-57 under 35 USC 103 over Scheidt in view of He and further in view of Shanton. Applicants respectfully submit that Scheidt does not teach or suggest a system having "a plurality of member tokens for providing cryptographic capabilities to authenticated users of the decentralized public network" as recited in claim 52. As previously described, Scheidt describes using a smart card or super card to stored this information in advance (Col. 9, lines 39-54) rather than distribute over a network. The Examiner supports this assertion and admits that Scheidt does not teach or suggest a method or system for distributing cryptographic capabilities over a decentralized public network. As previously described, these other cited references also does not teach, suggest or even describe any details related to key management or distributing cryptographic capabilities over a decentralized public network for at least the reasons previously described.

The Examiner also rejected Claims 21 and 22 under 35 USC 103 over Scheidt in view of He and Shanton and further in view of Win (US Pat 6,161,139) First, Claims 1,4, 7 and 52 remain patentable for at least the reasons specified previously as the Examiner has not established a prima

Applicant : Sweet et al.
Atty Dkt. : 00131-000100000
Issued : n/a
Serial No. : 09/930,029
Filed : 08/14/2001
Page : Page 26 of 28

facie case of obviousness. Consequently, dependant Claims 21 and 22 remain patentably distinct on their own as well as based upon their dependance on allowable independent claims.

Further, the Examiner also rejected Claim 58 under 35 USC 103 over Scheidt in view of He and Shanton and further in view of Anderson (US Pat 5,805,674). First, Claims 1,4, 7 and 52 remain patentable for at least the reasons specified previously, as the Examiner has not established a prima facie case of obviousness. Consequently, dependant Claim 58 remains patentably distinct on its own as well as based upon the dependance on allowable independent parent claims.

Applicant : Sweet et al.
Atty Dkt. : 00131-000100000
Issued : n/a
Serial No. : 09/930,029
Filed : 08/14/2001
Page : Page 27 of 28

In summary, Applicants respectfully request withdrawal of the rejections for claims 1-22, 52-66 and allowance of the claims as amended.

///

///

///

///

///

///

///

///

///

///

///

///

///

///

Applicant : Sweet et al.
Atty Dkt. : 00131-000100000
Issued : n/a
Serial No. : 09/930,029
Filed : 08/14/2001
Page : Page 28 of 28

The Applicant has made a diligent effort to place the claims in condition for allowance, should there remain unresolved issues that require adverse action, it is respectfully requested that the Examiner telephone Leland Wiesner, Applicants' Attorney at (650) 853-1113x 101 so that such issues may be resolved as expeditiously as possible.

For these reasons provided above, this application is now considered to be in condition for allowance and such action is earnestly solicited.

Respectfully Submitted,

June 19, 2009
Date


Leland Wiesner
Attorney/Agent for Applicant(s)
Reg. No. 39424

Wiesner and Associates
366 Cambridge Ave.
Palo Alto, California 94306
Tel. (650) 853-1113

Encl: Declaration, William B. Sweet